IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In Application of : **BAR et al.**

Serial No. : 10/774,169 : Group Art Unit: 2155

Filed : February 5, 2004 : Examiner: Thuong Nguyen

For : DETECTING AND PROTECTING AGAINST WORM TRAFFIC ON A NETWORK

PRE-APPEAL BRIEF REQUEST FOR REVIEW

I. Introductory Comments

Claims 1, 4-24, 29-35, 38-58, 63-69, 72-92 and 97-108 are pending in this application. Claims 1, 29, 32, 35, 63, 66, 69, 97 and 100 are independent claims.

On April 11, 2007, Appellant appealed from a final rejection of all the claims in this application and filed a Pre-Appeal Brief Request for Review (PABRR). Prosecution was then reopened with a new Official Action dated August 6, 2007, in which all of the pending claims were again rejected. In this Official Action, claims 1, 4-11, 21, 22, 25, 26, 28-35, 38-45, 55, 56, 59, 60, 62-69, 72-79, 89, 90, 93, 94, 96-103, 105 and 107 were rejected under 35 U.S.C. 103(a) over Lyle (U.S. Patent 6,886,102) in view of Givoly (U.S. Patent 7,099,940). Dependent claims 12-20, 23, 24, 46-54, 57, 58, 80-88, 91, 92, 104, 106 and 108 were rejected under 35 U.S.C. 103(a) over Lyle in view of Givoly and further in view of other references. Appellant has now filed an amendment canceling claims 25, 26, 28, 59, 60, 62, 93, 94 and 96 without prejudice in order to clarify the issues on appeal.

Appellant respectfully submits that the cited art fails to teach, or even to suggest, every element of the independent claims remaining in this application. Accordingly, Appellant requests that the application be allowed on the existing claims or, in the alternative, that prosecution on the merits of the claims be reopened with a new non-final Official Action.

II. Rejection of independent claims 1, 35 and 69 under 35 U.S.C. 103(a) over Lyle in view of Givoly

These claims recite a method, apparatus and software product for processing communication traffic that is directed to a group of addresses on a network, based on monitoring traffic that is directed to a subset of the group. The subset of the group of the addresses that is to be monitored is identified such that the addresses in the subset are expected to receive smaller amounts of the communication traffic than other addresses in the

group. The Examiner acknowledged in the Official Action (page 4, lines 4-7) that Lyle does not teach this claim limitation. In fact, Lyle neither teaches nor suggests any criterion for selection of ports or addresses to be monitored.

The Examiner went on to maintain that Givoly (col. 7, lines 22-24) teaches identifying a subset of the group of the addresses that are expected to receive smaller amounts of communication traffic. The cited passage, however, relates to "detecting a scan of a plurality of ports and/or Internet Protocol (IP) addresses." It says nothing about the amount of traffic each of the ports or addresses is expected to receive, and certainly has nothing to do with identifying or choosing to monitor certain addresses that are expected to receive smaller amounts of communication traffic, as recited in claims 1, 35 and 69. Although Givoly describes methods of monitoring accounting information that is received in a network (see col. 2, lines 52-62, for example), he is silent on the question of how or why certain addresses might be chosen for monitoring.

Thus, the Examiner has failed to point out even a hint of teaching or motivation in either Lyle or Givoly that would have led a person of ordinary skill in the art to choose any particular subset of addresses for monitoring, let alone the surprising choice of identifying low-traffic addresses for this purpose, as recited in claims 1, 35 and 69. Therefore, independent claims 1, 35 and 69 are patentable over the cited art.

III. Rejection of independent claims 29, 63 and 97 under 35 U.S.C. 103(a) over Lyle in view of Givoly

These claims recite a method, apparatus and software product in which communication traffic is monitored so as to detect packets indicative of a network communication failure that is characteristic of a worm infection. Upon detecting an increase in the rate of arrival of these packets, the communication traffic is filtered so as to remove communication traffic that is generated by the worm infection. Applicant pointed out in response to a previous Official Action and in the previous PABRR in this case that Lyle neither teaches nor suggests applying this sort of packet detection criterion. (See Appellant's Response to Official Action filed December 7, 2006, pages 6-7.)

Nevertheless, in the present Official Action (page 9, lines 4-5), the Examiner simply repeated her earlier assertion that Lyle teaches "detecting an increase in a rate of arrival of the packets that are indicative of the communication failure" in col. 10, line 60 – col. 11, line 1. This passage, however, relates only to detecting the "level or rate" of "certain types of

messages" (lines 55-56), without specifying the types of messages that are involved. Lyle makes no mention or suggestion of communication failures or how they should be handled, and does not even hint that packets indicative of such failures could be used in filtering worm-generated traffic as required by the present claims.

Givoly also says nothing about either worm infections or packets that are indicative of a communication failure in the network. The passages cited by the Examiner in Givoly (col. 6, lines 45-48, and col. 7, lines 18-21) propose only that information be discarded in order to prevent "failure of back-end systems" due to overload. As noted earlier, Givoly monitors accounting information (col. 2, lines 52-62). He lists attributes of the accounting information that might be analyzed (col. 4, lines 56-60), but neither teaches nor suggests detecting packets of any particular type, let alone detecting packets that are indicative of a communication failure that is characteristic of a worm infection, as recited in claims 29, 63 and 97.

Therefore, independent claims 29, 63 and 97 are patentable over the cited art.

IV. Rejection of independent claims 32, 66 and 100 under 35 U.S.C. 103(a) over Lyle in view of Givoly

These claims recite a method, apparatus and software product in which communication traffic on a network is monitored so as to detect ill-formed packets. The ill-formed packets are used in determining that at least a portion of the traffic has been generated by a worm infection. Appellant pointed out in the above-mentioned response of December 7, 2006, and in the previous PABRR that Lyle fails to relate in any way to whether packets are well formed or ill formed, and certainly does not suggest that detection of ill-formed packets might be used in determining that a worm infection has occurred.

Yet again the Examiner has simply repeated the previous grounds of rejection. In the present Official Action, the Examiner stated (page 10, lines 3-5) that in col. 7, lines 9-19, "Lyle discloses that the method of scanning the network for the suspicious data within the tracking system." The cited passage, however, says only that "the sniffers search for data indicating an actual or suspected attack... as described more fully below." Lyle goes on to describe a number of ways in which the sniffers may search for such attack-related data (see, for example, col. 10, lines 30-59). None of these ways has anything to do with ill-formation of packets.

Givoly, likewise, says nothing at all about whether packets are well formed or ill formed, and thus could not possibly be taken to suggest detecting or making any other use of ill-formed packets.

Therefore, independent claims 32, 66 and 100 are patentable over Lyle.

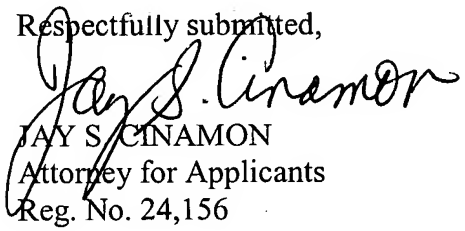
V. Rejection of the dependent claims

In view of the patentability of all the pending independent claims, as explained above, the dependent claims in this application are believed to be patentable, as well. Furthermore, notwithstanding the patentability of the independent claims, Appellant believes that the dependent claims recite independently-patentable subject matter. In the interest of brevity, however, Appellant will defer further argument regarding the dependent claims to the Appeal Brief, in the event that this application proceeds to appeal.

VI. Conclusion

In view of the above remarks, Appellant respectfully submits that all of the claims in the present application are in order for allowance. Notice to this effect is hereby requested.

Respectfully submitted,



JAY S. CINAMON
Attorney for Applicants
Reg. No. 24,156

ABELMAN, FRAYNE & SCHWAB
666 THIRD AVENUE, 10TH FLOOR
NEW YORK, NEW YORK 10017
Tel: (212) 949-9022
Direct: (212 885-9232
Fax: (212) 949-9190